



IT Security in Senior Living – How to keep your business and your residents secure

Christopher S Ellingwood, CISA, Principal

Agenda

- ▲ **1** Introduction
- ▲ **2** Network Attacks and Compliance
- ▲ **3** Educating Residents on Scams
- ▲ **4** Additional Resources for Educating Residents



Learning objectives



- ▲ To understand the security risks to senior living organizations
- ▲ Become aware of the scams impacting your residents
- ▲ Develop ways to educate your residents on risks
- ▲ Develop ways to protect your organization

Polling question

What percentage of nursing home patients use cell phones?

- a) 25%
- b) 5%
- c) 65%
- d) 85%





▲ Session 1

Introduction

Aging in Place

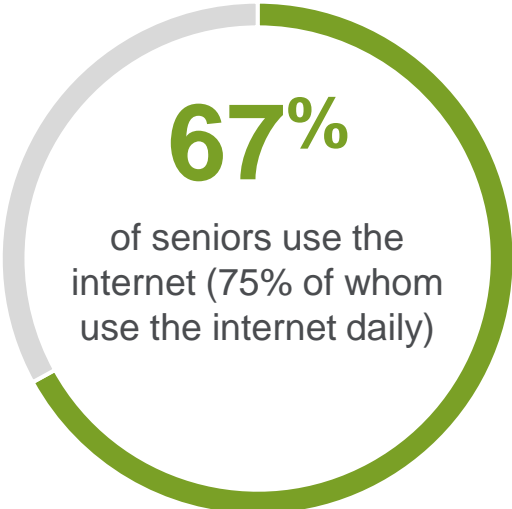
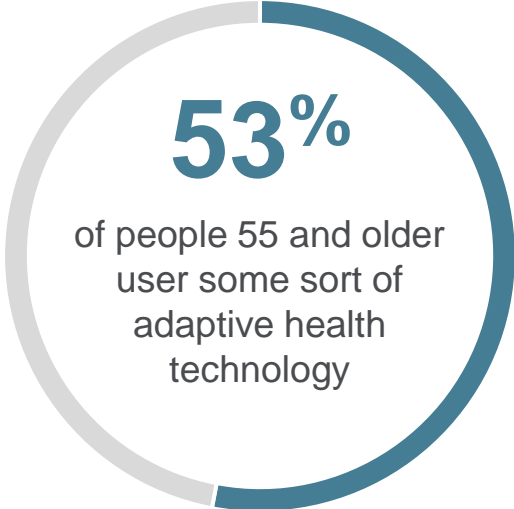
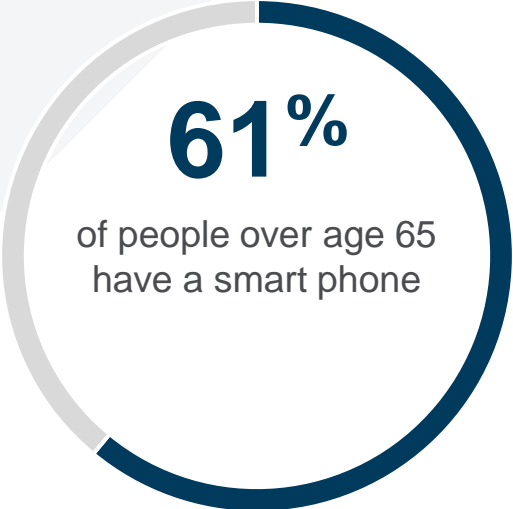
93% of people 55 and older agree that technology will aid them in aging in place (staying at home or in independent living communities longer).



Devices which have made it easiest to age in place

1. Medical or health-related mobile apps
2. Service-related apps (i.e. grocery delivery/food delivery apps)
3. Wearable medical or health-related trackers
4. Assistive smart home technologies
5. Hearing assistance-related devices
6. Medical alert system/devices

Technology Use by Seniors



Technology Use in Senior Living Organizations

- ▲ **1** Rapid increase in use of iPads, Amazon Echos, and Facebook for video calls and interaction for residents
- ▲ **2** Use of robotics, wearable technology, and sensors to help combat nursing shortages
- ▲ **3** Smart Home devices make the senior living experience more enjoyable and residents more independent
- ▲ **4** Digital/virtual caretakers, assistants, and doctor appointments
- ▲ **5** Nurses/doctors using bedside iPads, computers, and smart phones for charting and EMR access
- ▲ **6** Virtual reality for rehabilitation and mental engagement
- ▲ **7** Artificial intelligence for diagnosis and treatment





Session 2

Security Risks at Senior
Living Organizations

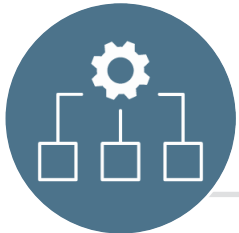
Why are Hackers Focusing on Senior Living?



Valuable and Sensitive Data (PHI)



Human Error



Limited Resources



Connected Systems



Vulnerabilities



Mobile Technology Environment



Physical Security



Vulnerable Residential Population

Polling question

What is the most common and effective way hackers conduct a successful attack?

- a) Ransomware
- b) Phishing Emails
- c) Denial of Service Attacks
- d) Cracking Passwords



Common Attack Example



Email Phishing

Leads to exposed data,
access to systems,
possible financial loss, etc.



Unauthorized Access



Ransomware / Malware

Risk!



TECH DAILY NEWS

Nurse call systems, other medical devices highest risks for cyberattacks: report

JOHN ROSZKOWSKI

MAY 3, 2023



In The News

 McKnight's Senior Living

Data breach leaked info on 40 nursing facilities, provider reports

A data breach over the summer may have given hackers access to health records for both residents and staff at 40 nursing homes.

2 days ago




 The New York Times

Ransomware Attack Disrupts Health Care Services in at Least Three States

It was not immediately clear how many locations operated by Prospect Medical Holdings were affected but some sites had to cut back services...

Aug 5, 2023



 HealthITSecurity

[Hawaii Skilled Nursing Facility Notifies 20K of Healthcare Data Breach](#)

March 07, 2023 - Aloha Nursing Rehab Centre, a skilled nursing facility in Kaneohe, Hawaii, notified 20,016 patients of a recent healthcare...

Mar 7, 2023





Protecting Systems

- ▲ Regular data backups that are encrypted
- ▲ Network segmentation
- ▲ Patch software
- ▲ Routine monitoring
- ▲ Separate guest/resident networks
- ▲ Multifactor authentication for medical systems
- ▲ Educate employees on risks and test
- ▲ Physical security controls
- ▲ Take away administrator rights of users
- ▲ Encrypt data at rest and in transit

HIPAA Compliance

HIPAA has teeth now, it's a good time to revisit your compliance

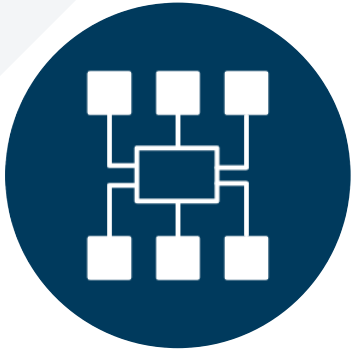
- ▲ Not just covered entities
- ▲ Training employees
- ▲ Disclosure
- ▲ Business associate agreements
- ▲ Understand the requirements of the security, breach, and privacy rules
- ▲ OCR now doing audits and fines



Important Controls Related for HIPAA



Impacts of an Attack



Compromised Network

Locked out from networks



Data Loss

Data breach and costs associated with that



Financial Loss

Inability to provide patient care



Session 3

Educating Residents on Scams

Teaching Your Residents about Scams and Internet Safety is as Important as Treating their Health

Polling question

What is the most common way seniors fall victim to fraudulent scams?

- a) Government Imposters (IRS/Social Security)
- b) “Grandma help, I’m in trouble” scam
- c) Looking for Love in all the Wrong Places
- d) Email Phishing
- e) Mail (Letters) Scams



Scams Online are Common

- ▲ The FBI estimates that seniors lose almost \$30 billion a year annually to scams
- ▲ Average senior individual loss was \$34,000



More Stats!

- ▶ The most common way scammers are successful: asking for gift cards
- ▶ 400% increase in cybercrimes in the last five years
- ▶ Seniors are the least likely age group to report fraud or a scam

Identity Theft Types

| Rank | Theft Type | # of Reports |
|------|--|--------------|
| 1 | Government Documents or Benefits Fraud | 406,375 |
| 2 | Credit Card Fraud | 393,207 |
| 3 | Other Identity Theft | 353,152 |
| 4 | Loan or Lease Fraud | 204,967 |
| 5 | Employment or Tax-Related Fraud | 113,529 |
| 6 | Phone or Utilities Fraud | 99,539 |
| 7 | Bank Fraud | 89,476 |





How We Educate Residents

Sample slides and content for residents, but information anyone in Senior Living should be aware of!

Example 1

From: Amazon <management@mazoncanada.ca> on behalf of Amazon not an Amazon email address (note the missing A in Amazon) 05/01/2014 7:55 PM
To: @sheridanc.on.ca
Cc:
Subject: Suspension

amazon.com

Dear Client, ← Generic non-personalized greeting


We have sent you this e-mail, because we have strong reason to believe, your account has been used by someone else. In order to prevent any fraudulent activity from occurring we are required to open an investigation into this matter. We've locked your Amazon account, and you have 36 hours to verify it, or we have the right to terminate it.

To confirm your identity with us click the link below:

<https://www.amazon.com/exec/obidos/sign-in.html>

Sincerely, ↗ Hovering over the link reveals it points to a non-Amazon site - "http://redirect.kereskedj.com"

The Amazon Associates Team



© 1996-2013, Amazon.com, Inc. or its affiliates

Example 2

Two screenshots of text messages illustrating smishing attacks. The left message is from +1 (347) 267-4843, dated Tue, Sep 14, 10:42 AM, and contains a link to k8bvz.info/Ask3AqghsD. The right message is from +1 (518) 982-4819, dated Thu, Apr 8, 3:53 AM, and contains a link to ut08y.com/HmDZ5FqvE6. Red boxes highlight the links, and red arrows point from them to a summary box at the bottom.

Smishing attacks use a variety of tactics to get users to click on unsafe links









Educating Residents

- ▲ Be patient and understanding
- ▲ Make it easy to communicate
- ▲ Inform them frequently
- ▲ Don't scare them away



Educating Residents: Social Media

- ▲ Keep Accounts Private
- ▲ Don't Accept All Friend Requests
- ▲ Use Unique Passwords
- ▲ Special Characters and Numbers (@,!,22)

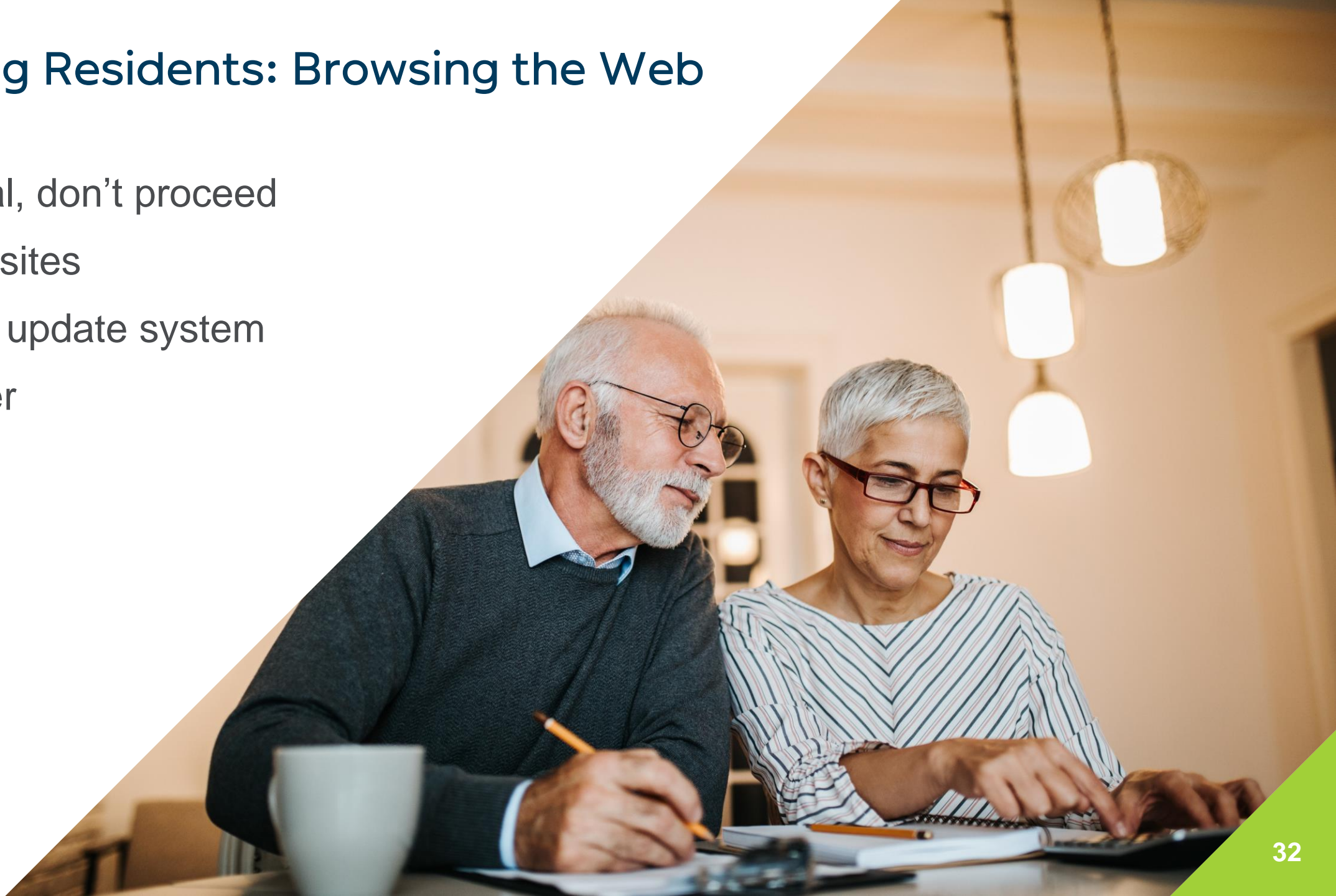


Educating Residents: Dating Sites

- ▲ Be Cautious
- ▲ Don't Give Out Personal Info
- ▲ Ask to Video Chat
- ▲ Find Love!

Educating Residents: Browsing the Web

- ▲ If skeptical, don't proceed
- ▲ Common sites
- ▲ Regularly update system
- ▲ Ad-blocker





Session 4

Additional Resources for
Educating Residents

FTC Videos: Cyber Safety

Questions?

Christopher Ellingwood

207.541.2290

cellingwood@berrydunn.com



berrydunn.com